

Eisenstein の積公式の種数 2 への一般化について

大西良博 (YOSHIHIRO ÔNISHI)

東京都立大学理学部
(Department of Mathematics, Faculty of Science,
Tokyo Metropolitan University)

0. はじめに

p を奇素数とするとき公式

$$(0.1) \quad \prod_{r=1}^{p-1} 2\sqrt{-1} \sin \frac{2\pi r}{p} = p$$

はよく知られている. これを楕円函数に一般化する公式は最初は恐らく Eisenstein によって扱われた. その例として以下の様な公式がある. affine な方程式が

$$(0.2) \quad y^2 = x^3 + \frac{1}{4}$$

で与えられるような楕円曲線 E は $\mathbb{Z}[\zeta_3]$, $\zeta_3 = e^{\frac{2\pi\sqrt{-1}}{3}}$ を自己同型環として持ち, 素元

$$\varpi \in \mathbb{Z}[\zeta_3], \equiv 1 \pmod{(1-\zeta_3)^2}$$

について ϖ -等分点の全体 ϖE は $p = N\varpi$ 個の元から成るが, このとき

$$(0.3) \quad \prod_{P \in \varpi E, P \neq O} x(P) = \frac{1}{\varpi^2}$$

が成り立つ. ここで $x(P)$ は P の方程式 (0.1) での x -座標, O は E の群としての単位元である.

これらの公式を扱う動機の一つとして Gauss の和の符号決定問題があることは言うまでもない ([M1], [M2]).

I. 目的

この講演の目的は David Grant によって発見された積公式, 即ち (1), (2) を種数 2 の曲線に一般化する公式を紹介し, 併せてその積に現れる座標が生成する体の Galois 群についての講演者による数値実験の結果を述べることにある.

II. 種数 2 の曲線 (RIEMANN 面) 上の函数論 (H.F. BAKER の仕事)

Grant の公式 (3.2) を述べるために超楕円曲線及びそれらの Jacobi 多様体上の Abel 函数論について以下で必要な場合に限ってその概略を述べる. それらは Weierstrass の仕事を元に H. F. Baker が整備したものである. ([B1],[B2]).

a. Jacobi 多様体の代数的理論.

いま C を affine な方程式が

$$(2.1) \quad y^2 = x^5 + \frac{1}{4}$$

で表される射影的で smooth な C 上定義された代数曲線とし, J をその Jacobi 多様体とする. J には C の 2 次対称積 $\text{Symm}^2 C$ から J への全射

$$\begin{aligned} \varphi: \text{Symm}^2 C &\rightarrow J \\ (P_1, P_2) &\mapsto P_1 + P_2 - 2\infty \end{aligned}$$

があり, これは丁度 J の単位元での blowing up になっている. そこで J 上の函数は $\text{Symm}^2 C$ の点 $((x_1, y_1), (x_2, y_2))$ を用いてその対称式として表すことが多い. また

$$\begin{aligned} \iota: C &\hookrightarrow J \\ P &\mapsto P + \infty \end{aligned}$$

なる埋め込みの像を θ で表す. $\zeta := e^{\frac{2\pi\sqrt{-1}}{5}}$ とするとき C には $-\zeta$ が

$$[-\zeta](x, y) = (\zeta x, -y)$$

によって作用しているから J には φ を通じて $\mathbb{Z}[\zeta]$ が作用している.

b. Jacobi 多様体の解析的理論.

C 上の正則な 1-形式の層 Ω_C^1 の基を

$$\omega_1 = \frac{dx}{y}, \quad \omega_2 = \frac{x dx}{y}.$$

と取り, 第 3 種微分形式の層の基底

$$\eta_1 = \frac{3x^3}{2y} dx, \quad \eta_2 = \frac{x^2}{2y} dx$$

をとる. 下の図のように C の積分路 $\alpha_1, \alpha_2, \beta_1, \beta_2$ をとり, 周期行列

$$\begin{aligned} \Omega_1 &= \begin{bmatrix} \int_{\alpha_1} \omega_1 & \int_{\alpha_2} \omega_1 \\ \int_{\alpha_1} \omega_2 & \int_{\alpha_2} \omega_2 \end{bmatrix} = \begin{bmatrix} 2K_1(\zeta^3 - \zeta^4) & 2K_1(\zeta - \zeta^2) \\ 2K_2(\zeta - \zeta^3) & 2K_2(\zeta^2 - \zeta^4) \end{bmatrix} \\ \Omega_2 &= \begin{bmatrix} \int_{\beta_1} \omega_1 & \int_{\beta_2} \omega_1 \\ \int_{\beta_1} \omega_2 & \int_{\beta_2} \omega_2 \end{bmatrix} = \begin{bmatrix} 2K_1(-1 + \zeta - \zeta^2 + \zeta^3) & 2K_1(\zeta - 1) \\ 2K_2(-1 + \zeta^2 - \zeta^4 + \zeta) & 2K_2(\zeta^2 - 1) \end{bmatrix} \end{aligned}$$

を定める. ここに

$$\begin{aligned}
 K_1 &= \int_{(0, \frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}}, 0)} \omega_1 \\
 &= -0.95015013898843674150305765442105298951 \dots, \\
 K_2 &= \int_{(0, \frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}}, 0)} \omega_2 \\
 &= 0.42261692031717290436050061364858957077 \dots.
 \end{aligned}$$

さらに擬周期行列を

$$\eta = \begin{bmatrix} \int_{\alpha_1} \eta_1 & \int_{\alpha_1} \eta_2 \\ \int_{\alpha_2} \eta_1 & \int_{\alpha_2} \eta_2 \end{bmatrix} = \begin{bmatrix} 2H_1(\zeta^2 - \zeta) & 2H_1(\zeta^4 - \zeta^3) \\ 2H_2(\zeta^4 - \zeta^2) & 2H_2(\zeta^3 - \zeta) \end{bmatrix}$$

で定める. ここに

$$\begin{aligned}
 H_1 &= \int_{(0, \frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}}, 0)} \omega_1 \\
 &= \sqrt{(-1)} \cdot 0.45508926983787695734043475371247514671 \dots, \\
 H_2 &= \int_{(0, \frac{1}{2})}^{(-\sqrt[5]{\frac{1}{4}}, 0)} \omega_2 \\
 &= -\sqrt{(-1)} \cdot 0.24153442080024718212596751624538334733 \dots.
 \end{aligned}$$

簡単な計算により C の modulus τ は

$$\tau = \Omega_1^{-1} \Omega_2 = \begin{bmatrix} 1 - \zeta^4 & -\zeta^2 - \zeta^4 \\ -\zeta^2 - \zeta^4 & \zeta \end{bmatrix}$$

となる. このとき C から定まる超楕円 sigma 関数が

$$(2.2) \quad \sigma(u) = c \exp\left(-\frac{1}{2} u \eta \Omega_1^{-1} {}^t u\right) \vartheta \begin{bmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \end{bmatrix} (\Omega_1^{-1} {}^t u; \tau)$$

で定義される. ここに

$$\begin{aligned}
 u &= (u_1, u_2), \\
 u_1 &= \int_{(\infty, \infty)}^{(x_1, y_1)} \omega_1 + \int_{(\infty, \infty)}^{(x_2, y_2)} \omega_1, \\
 u_2 &= \int_{(\infty, \infty)}^{(x_1, y_1)} \omega_2 + \int_{(\infty, \infty)}^{(x_2, y_2)} \omega_2
 \end{aligned}$$

は J を 2 次元の複素トーラスとして解析的多様体と考えたときの原点における標準的な局所座標であり定数 c は

$$\begin{aligned} c &= 5^{5/8} \frac{\sqrt{\det(\Omega_1)}}{2\pi} \\ &= 5^{5/8} \frac{\sqrt{(K_1 K_2 (1-\zeta)(1-\zeta^2)^2)}}{\pi} \\ &= 1.137461223393266128486448504150004558 \dots, \end{aligned}$$

で与えられる ([G1] 参照). さらに $i, j, k \in \{1, 2\}$ に対して

$$\begin{aligned} (2.3) \quad \rho_{ij}(u) &= \frac{\partial^2}{\partial u_i \partial u_j} \sigma(u), \\ \rho_{ijk}(u) &= \frac{\partial}{\partial u_k} \rho_{ij}(u), \end{aligned}$$

$$(2.4) \quad \sigma_2(u) = \frac{\partial}{\partial u_2} \sigma(u)$$

とおく. このとき楕円関数の時のように $u, v \in J - \Theta$ に対して

$$(2.5) \quad -\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = \rho_{11}(u) - \rho_{11}(v) + \rho_{12}(u)\rho_{22}(v) - \rho_{22}(u)\rho_{12}(v)$$

なる式が成り立って ([B2]), これより $\rho_{ij}(u)$ らの代数的加法公式が得られる ([B1, G3]).

また $\alpha \in \mathbb{Z}[\zeta]$ に対して $N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})}(\alpha) = n_\alpha + m_\alpha \varepsilon^2$ とし, $\varepsilon = 1 + \zeta + \zeta^4$ とするとき

$$(2.6) \quad \psi_\alpha(u) = \frac{\sigma(\alpha u)}{\sigma_2(u)^{n_\alpha} (-\sigma(\varepsilon u))^{m_\alpha}}.$$

が Weber の psi 関数の良い一般化になっている ([G3, §3] 参照). さて [G3] に従って

$$(2.7) \quad X(u) = \frac{1}{2} (\rho_{11}(u)\rho_{22}(u) - \rho_{12}(u)^2)$$

とおくと

$$(2.8) \quad X(u) = \frac{\sigma(u+P)\sigma(u+2P)\sigma(u-3P) + \sigma(u-P)\sigma(u-2P)\sigma(u+3P)}{2\sigma(u)^3\sigma_2(P)\sigma(2P)\sigma(-3P)},$$

と σ 関数を使って表される. ここに $P = i(0, \frac{1}{2})$ であり, X は

$$(2.9) \quad X(-\zeta u) = \zeta^4 X(u)$$

なる性質を持つ.

III. GRANT の公式

いま

$$(3.1) \quad G(\beta) = \{Q = \iota(x, y); \text{Im} y > 0, Q \in \Theta \cap [\beta\beta^{\sigma^{-1}}]^*(X)_0, 2Q \neq O\}$$

とおく. ここで $(X)_0$ は函数 X の零点因子であり, O は J の単位元である. 因子 Θ の自己交点数は 2 であり $(X)_0$ は 3Θ と線形同値であるから $\#G(\beta) = 3(p-1)$ ([G3, Remark]). 以上の準備のもとに Grant の公式は次のように述べられる:

定理 3.2.

$$\prod_{Q \in G(\beta)} x(\iota^{-1}(Q)) = \frac{1}{\beta\beta^{\sigma}}.$$

注意.

$G(\beta)$ に属する点はすべて J の群構造に関して捻れが無い事がわかる ([G3] 参照). しかし同様の定義を楕円曲線の場合に行えば従来の等分点に一致する.

IV. $G(\beta)$ が生成する GALOIS 群について

さて $\{x(Q); Q \in G(\beta)\}$ が $\mathbb{Q}(\zeta)$ 上に生成する体拡大について調べるために

$$(4.1) \quad \Phi(\beta; T) = \prod_{Q \in G(\beta)} (T - \frac{1}{x(Q)}) \in \mathbb{Q}[\zeta][T],$$

とおく. このとき [G3, §4] により,

$$(4.2) \quad x(u)^{3(p-1)} \Phi(\beta; \frac{1}{x(u)}) = \frac{(-1)^{N\beta-1} X(\beta\beta^{\sigma^{-1}}u) (\psi_{\beta\beta^{\sigma^{-1}}}(u))^3}{y(u)}$$

が成り立つ. ここで T は不定元である. $\mathbb{Z}[\zeta]$ の作用から, 多項式 $\Psi(\beta; S) \in \mathbb{Q}[\zeta][S]$ (ここで S も不定元) が存在して

$$(4.3) \quad \Phi(\beta; T) = \Psi(\beta; T^5)$$

をみかす. そこで $\Phi(\beta; T)$ 及び $\Psi(\beta; S)$ の $\mathbb{Q}(\zeta)$ 上のそれぞれの分解体を $L_\beta = \mathbb{Q}(x(Q); P \in G(\beta))$ 及び $K_\beta = \mathbb{Q}(x(Q)^5; Q \in G(\beta))$ とし,

$$(4.4) \quad \{\zeta^\nu \alpha_j\} \quad (\nu = 0, \dots, 4; j = 1, \dots, \frac{3(p-1)}{5})$$

を $\Phi(\beta; T) = 0$ の根の全体とする. このとき $\text{Gal}(L_\beta/\mathbb{Q}(\zeta))$ は上の根の置換群 ($\mathcal{G}_\beta$ と名付ける) の部分群と考えられる. $\mathcal{G}_\beta$ は次の 2 種類の置換から生成される. すなわち

$$(4.5) \quad \langle i_1, i_2, \dots, i_{\frac{3(p-1)}{5}} \rangle : \alpha_\nu \mapsto \zeta^{i_\nu} \alpha_\nu \text{ for all } \nu,$$

と互換

$$(4.6) \quad (ij) : \zeta^\nu \alpha_i \mapsto \zeta^\nu \alpha_j, \zeta^\nu \alpha_k \mapsto \zeta^\nu \alpha_k \quad (\nu = 0, 1, \dots, 4; k \neq i, j)$$

からである. 講演者は $G(\beta)$ にはその Galois 群を統制するような構造 (楕円曲線の場合の F_p 加群の構造などに対応するもの) が無いと思われることから次のような予想を立ててみた.

予想 4.7.

任意の素元 $\beta \equiv \pm 1 \pmod{(1-\zeta)^2}$ について $N\beta = p$ と書く. 体 L_β 及び群 G_β は上のとおりとする. このとき

$$\text{Gal}(L_\beta/\mathbb{Q}(\zeta)) = G_\beta$$

となっているであろう.

さらに $N\beta=11, 31, 41, 61$ なる β について本稿の最後にある Table 1 のように $\Phi(\beta; T)$ を UBASIC を用いて計算してみたが, その結果この予想がこれらについては成り立つことがわかった. 以下その計算方法について略述し, 若干の注意を述べる.

V. $\Phi(\beta; T)$ は $\mathbb{Z}[\zeta]$ に属するか?

命題 5.1.

$$\Phi(\beta; T) \in \mathbb{Z}[\frac{1}{2}][\zeta].$$

証明. ([G3, Remark (1) in the introduction]). いま p の上にある L_β の素イデアル $\mathfrak{P}$ に対して $x(Q) \equiv 0 \pmod{\mathfrak{P}}$ であるとする. これは例えば non-Weierstrass 点が Weierstrass 点に degenerate することを意味するから, $\mathfrak{P}$ は bad reduction prime である. 従って p は 10 を割る. 一方, もし $x(Q)^{-1} \equiv \pmod{\mathfrak{P}}$ とすると,

$$t_2(Q)^2 = \frac{y(Q)^2}{x(Q)^6} = \frac{1}{x(Q)} + \frac{1}{2x(Q)^6},$$

であることによって $\mathfrak{P}$ は $2\beta\beta^\sigma$ を割る. よって $x(Q)^{-1}$ ($Q \in G(\beta)$) は 2 を割らない任意の素点において整である. ■

一般に $\Phi(\beta; T)$ が $\mathbb{Z}[\zeta]_{(2)}$ 上でも定義されるか否かはわかっていないが, いくつかの β についてはそうなることが以下のようにしてわかる. すなわち, まず Weber が Argebra III で用いた方法 ([T, p.145], [F, p.184]) に基付き, 前に定義した $\phi_\alpha(u)$ の α に関する漸化式が (2.5) から導かれる

$$(5.2) \quad -\frac{\psi_{\alpha+\beta}(u)\psi_{\alpha-\beta}(u)}{\psi_\alpha(u)^2\psi_\beta(u)^2} + \rho_{11}(\beta u) = -\rho_{11}(\alpha u) + \rho_{12}(\alpha u)\rho_{22}(\beta u) - \rho_{22}(\alpha u)\rho_{12}(\beta u).$$

により得られる. 漸化式から $\phi_\alpha(u)$ が $\mathbb{Z}_{(2)}[\zeta]$ 上整であることがわかる. 一方 $\sigma(u)$ の, C の座標でいえば (∞, ∞) 及び $(0, \pm\frac{1}{2})$ に於ける Taylor 展開から $\phi_{\beta\beta^{-1}}(u)$ の最高次係数と定数項がわかる. そこで Θ 上 $x(u)$ の多項式として $\mathbb{Z}[\zeta]_{(2)}$ 上原始的であることがその 2 係数からわかる場合は $X(\beta\beta^{\sigma^{-1}}u)$ の分母としての (see. [O]) $\Phi(\beta; T)$ が $\mathbb{Z}[\zeta]_{(2)}$ 上整であることが次のことからわかる.

$$\begin{aligned} & y(u)x(u)^{3(p-1)}\Phi(\beta; x(Q)^{-1})\psi_\alpha(u) \\ &= \psi_\alpha(u)^4 X(\alpha u) \\ (5.3) \quad &= \frac{1}{2} \{ \rho_{11}(\alpha u)\psi_\alpha(u)^2 \rho_{22}(\alpha u)\psi_\alpha(u)^2 - (\rho_{12}(\alpha u)\psi_\alpha(u)^2)^2 \} \\ &\in \mathbb{Z}[\zeta]_{(2)}[x(Q)]. \end{aligned}$$

特に Table 1 にある $N\beta = 11, 31, 41, 61$ の場合は $\Phi(\beta; T)$ は $\mathbb{Z}[\zeta]$ 上整である.

VI. $\Phi(\beta; T)$ の近似計算

$\psi_\alpha(u)$, $X(u)$ の定義と(5.3)式からわかるように $\Phi(\beta, x(Q)^{-1})$ は $\sigma(u)$ や $\sigma_2(u)$ の特殊値で書けるが, フーリエ級数であるそれらは収束が早く非常に精密な近似値が得られる. よって次数が小さいとき, つまり $N\beta - 1$ が小さいときは補間法により $\Phi(\beta, T)$ が求められる.

VII. GALOIS 群の計算

適当な素イデアルで reduction (Table 2) して, 次の補題を用いれば, これら 4 つの場合についてはさきの予想が正しいことがわかる. (2つの)

命題 7.1.

H を n 次対称群 S_n の部分群とする. もし H が互換と長さ n 及び $n-1$ の巡回置換を含むならば H は S_n に一致する.

命題 7.2.

$f(T) \in \mathbb{Z}[\zeta][T]$ をモニックな n 次分離的多項式とする. ϖ of $\mathbb{Z}[\zeta]$ の素元 ϖ を一つとって固定する. もし $f(T) \bmod \varpi$ が $\mathbb{Z}[\zeta][T]/(\varpi)$ 上で次数 $r_1, r_2, \dots, r_s$ の多項式の積に分解するならば, $f(T)$ の Galois 群は $(r_1, r_2, \dots, r_s)$ 型の置換を含む.

REFERENCES

- [B1] H.F. Baker, "An Introduction to the Theory of Multiply Periodic Functions," Cambridge, 1907.
- [B2] H.F. Baker, *On the hyperelliptic sigma functions*, Amer. J. of Math. XX (1898), 301-384.
- [F] R. Fricke, "Die elliptischen Functionen und ihre Anwendungen, II," 1922.
- [G1] D. Grant, *On a generalization of Jacobi's derivative formula to dimension two*, J. reine angew. Math. 392 (1988), 125-136.
- [G2] D. Grant, *Formal groups in genus two*, J. reine angew. Math. 411 (1990), 96-121.
- [G3] D. Grant, *A generalization of a formula of Eisenstein*, J. London Math. Soc. (1991) (to appear).
- [M1] C. R. Matthews, *Gauss sums and elliptic functions : I. The kummer Sum*, Invent. math. 52 (1979), 163-185.
- [M2] C. R. Matthews, *Gauss sums and elliptic functions : II. The Quartic Sum*, Invent. Math. 54 (1979), 23-52.
- [O] Y. Ônishi, *Some examples of the formula of Grant*.
- [T] 竹内端三, "楕圓函數論," 岩波全書, 1936.

Table. 1

$$p=11, \beta=1-\sqrt{5}\zeta$$

$$\begin{aligned} & \Phi(1-\sqrt{5}\zeta; T^{-1})T^{90} \\ & = (2\zeta + 0\zeta^2 - 2\zeta^3 + 1\zeta^4)T^{90} \\ & + (481\zeta + 608\zeta^2 + 81\zeta^3 + 31\zeta^4)T^{85} \\ & + (755\zeta + 8850\zeta^2 + 1545\zeta^3 + 790\zeta^4)T^{80} \\ & + (-1045\zeta + 8190\zeta^2 + 850\zeta^3 - 440\zeta^4)T^{75} \\ & + (-235\zeta - 105\zeta^2 + 750\zeta^3 - 370\zeta^4)T^{70} \\ & + (43\zeta + 85\zeta^2 + 23\zeta^3 - 11\zeta^4)T^{65} \\ & + 1 \end{aligned}$$

$$p=31, \beta=2\zeta - \zeta^2$$

$$\begin{aligned} & \Phi(2\zeta - \zeta^2; T^{-1})T^{90} \\ & = (3\zeta + 2\zeta^2 + 8\zeta^3 + 0\zeta^4)T^{90} \\ & + (49130\zeta + 63127\zeta^2 + 52114\zeta^3 + 72021\zeta^4)T^{85} \\ & + (72513886\zeta - 95597055\zeta^2 - 32596268\zeta^3 - 180457587\zeta^4)T^{80} \\ & + (5336335946\zeta + 2959913601\zeta^2 - 1703408144\zeta^3 + 1687387536\zeta^4)T^{75} \\ & + (-14754715590\zeta - 7740236770\zeta^2 - 56603191800\zeta^3 - 56429781880\zeta^4)T^{70} \\ & + (-23652059209\zeta + 82899543704\zeta^2 + 25939829052\zeta^3 - 129958384345\zeta^4)T^{65} \\ & + (-1101355052300\zeta - 887460640566\zeta^2 - 895659713302\zeta^3 - 912140700173\zeta^4)T^{60} \\ & + (-1077203581153\zeta - 1518111474740\zeta^2 - 1110674418717\zeta^3 - 1353475398839\zeta^4)T^{55} \\ & + (-896583135093\zeta - 1059408992478\zeta^2 - 936337020063\zeta^3 - 713174075123\zeta^4)T^{50} \\ & + (-502120589520\zeta - 381550846985\zeta^2 - 622101740750\zeta^3 - 444344021415\zeta^4)T^{45} \\ & + (-173127443291\zeta + 51718893939\zeta^2 - 197074499722\zeta^3 - 176927885810\zeta^4)T^{40} \\ & + (-31260272990\zeta + 5439329351\zeta^2 - 21680088963\zeta^3 - 29969845017\zeta^4)T^{35} \\ & + (-926085302\zeta + 424750620\zeta^2 + 582306632\zeta^3 - 186588381\zeta^4)T^{30} \\ & + (769436648\zeta - 104755497\zeta^2 + 579468833\zeta^3 + 384254463\zeta^4)T^{25} \\ & + (103268235\zeta - 26994995\zeta^2 + 66571300\zeta^3 + 18930170\zeta^4)T^{20} \\ & + (4044997\zeta - 2352267\zeta^2 + 1248164\zeta^3 - 858295\zeta^4)T^{15} \\ & + (19910\zeta - 80662\zeta^2 - 68724\zeta^3 + 43169\zeta^4)T^{10} \\ & + (89\zeta - 75\zeta^2 + 726\zeta^3 + 1662\zeta^4)T^5 \\ & + 1 \end{aligned}$$

$$p=41, \quad \beta = \zeta^2 + 2\zeta^3 + 3\zeta^4$$

$$\begin{aligned} & \Phi(\zeta^2 + 2\zeta^3 + 3\zeta^4; T^{-1}) T^{128} \\ = & \quad (-2\zeta + \quad \quad \quad 2\zeta^2 - \quad \quad \quad 4\zeta^3 - \quad \quad \quad 5\zeta^4) T^{128} \\ + & \quad (24807\zeta - \quad \quad \quad 68475\zeta^2 - \quad \quad \quad 154652\zeta^3 - \quad \quad \quad 22369\zeta^4) T^{116} \\ + & \quad (-1035129149\zeta + \quad \quad \quad 4250240268\zeta^2 + \quad \quad \quad 1256418780\zeta^3 + \quad \quad \quad 1766313157\zeta^4) T^{110} \\ + & \quad (384381706505\zeta + \quad \quad \quad 224046288058\zeta^2 + \quad \quad \quad 221479332942\zeta^3 + \quad \quad \quad 81727059798\zeta^4) T^{105} \\ + & \quad (10822902349869\zeta - \quad \quad \quad 17336069898736\zeta^2 - \quad \quad \quad 752514987516\zeta^3 - \quad \quad \quad 16248580066398\zeta^4) T^{100} \\ + & \quad (55420294345053\zeta + \quad \quad \quad 45974992436357\zeta^2 - \quad \quad \quad 139934783318974\zeta^3 - \quad \quad \quad 25874298892050\zeta^4) T^{95} \\ + & \quad (962680198843117\zeta + \quad \quad \quad 1312717533007740\zeta^2 + \quad \quad \quad 859558673820393\zeta^3 + \quad \quad \quad 566842474863108\zeta^4) T^{90} \\ + & \quad (6414290801515241\zeta + \quad \quad \quad 5242565955772993\zeta^2 + \quad \quad \quad 4500468875803315\zeta^3 + \quad \quad \quad 2196172741942577\zeta^4) T^{85} \\ + & \quad (7050363148188925\zeta - \quad \quad \quad 1763240405962434\zeta^2 + \quad \quad \quad 1269991312395817\zeta^3 - \quad \quad \quad 150995999031162\zeta^4) T^{80} \\ + & \quad (14467648987103144\zeta - \quad \quad \quad 4866798898025541\zeta^2 - \quad \quad \quad 3424006173521701\zeta^3 - \quad \quad \quad 2019299768848561\zeta^4) T^{75} \\ + & \quad (17237482028292803\zeta - \quad \quad \quad 2322168805999833\zeta^2 - \quad \quad \quad 1095116726199179\zeta^3 - \quad \quad \quad 1789095816693445\zeta^4) T^{70} \\ + & \quad (9411820041030182\zeta + \quad \quad \quad 709299803466255\zeta^2 - \quad \quad \quad 1495144619378142\zeta^3 + \quad \quad \quad 39532042053398\zeta^4) T^{65} \\ + & \quad (3011692630803171\zeta + \quad \quad \quad 615305832612413\zeta^2 - \quad \quad \quad 1076718879003750\zeta^3 + \quad \quad \quad 255271885050577\zeta^4) T^{60} \\ + & \quad (780416588154445\zeta + \quad \quad \quad 631202072478341\zeta^2 + \quad \quad \quad 195831864131897\zeta^3 + \quad \quad \quad 521395954860073\zeta^4) T^{55} \\ + & \quad (165732471606804\zeta + \quad \quad \quad 337884308703789\zeta^2 + \quad \quad \quad 312420131959074\zeta^3 + \quad \quad \quad 320333682043184\zeta^4) T^{50} \\ + & \quad (28117825910893\zeta + \quad \quad \quad 70909058240587\zeta^2 + \quad \quad \quad 84635622002171\zeta^3 + \quad \quad \quad 84654838681810\zeta^4) T^{45} \\ + & \quad (6596859551682\zeta + \quad \quad \quad 3608103383795\zeta^2 + \quad \quad \quad 8000311210588\zeta^3 + \quad \quad \quad 15347056749618\zeta^4) T^{40} \\ + & \quad (1164234227031\zeta - \quad \quad \quad 160939539252\zeta^2 + \quad \quad \quad 446105663060\zeta^3 + \quad \quad \quad 1844506446612\zeta^4) T^{35} \\ + & \quad (47587057890\zeta + \quad \quad \quad 12774161398\zeta^2 + \quad \quad \quad 90855113862\zeta^3 + \quad \quad \quad 51760084148\zeta^4) T^{30} \\ + & \quad (-13827072116\zeta - \quad \quad \quad 3470278388\zeta^2 + \quad \quad \quad 6777725144\zeta^3 - \quad \quad \quad 15009421976\zeta^4) T^{25} \\ + & \quad (-1125729797\zeta - \quad \quad \quad 142964613\zeta^2 + \quad \quad \quad 408778486\zeta^3 - \quad \quad \quad 1151049435\zeta^4) T^{20} \\ + & \quad (-17315413\zeta - \quad \quad \quad 304940\zeta^2 + \quad \quad \quad 21867438\zeta^3 - \quad \quad \quad 14365624\zeta^4) T^{15} \\ + & \quad (124331\zeta + \quad \quad \quad 247953\zeta^2 + \quad \quad \quad 537345\zeta^3 + \quad \quad \quad 240827\zeta^4) T^{10} \\ + & \quad (1810\zeta + \quad \quad \quad 2268\zeta^2 + \quad \quad \quad 3607\zeta^3 + \quad \quad \quad 2143\zeta^4) T^5 \\ + & 1 \end{aligned}$$

$$i=61, \beta=3\zeta^2+\zeta^4$$

$$\Phi(3\zeta^2+\zeta^4; T^{-1})T^{180}$$

$$\begin{aligned} & \cdot (\quad \quad \quad 6\zeta - \quad \quad \quad 2\zeta^2 + \quad \quad \quad 0\zeta^3 - \quad \quad \quad 3\zeta^4)T^{180} \\ & \cdot (\quad \quad \quad 2049678\zeta + \quad \quad \quad 983466\zeta^2 - \quad \quad \quad 804194\zeta^3 + \quad \quad \quad 278071\zeta^4)T^{175} \\ & \cdot (\quad \quad \quad 181304340245\zeta + \quad \quad \quad 52262734570\zeta^2 - \quad \quad \quad 189570157255\zeta^3 + \quad \quad \quad 65417648445\zeta^4)T^{170} \\ & \cdot (- \quad \quad \quad 57588214192215\zeta - \quad \quad \quad 18033404398520\zeta^2 - \quad \quad \quad 152982856122000\zeta^3 - \quad \quad \quad 97593828395880\zeta^4)T^{165} \\ & \cdot (\quad \quad \quad 14716157389618050\zeta - \quad \quad \quad 5598589439456770\zeta^2 + \quad \quad \quad 18810382591544680\zeta^3 - \quad \quad \quad 22226814611875585\zeta^4)T^{160} \\ & \cdot (- \quad \quad \quad 281501150548488347\zeta + \quad \quad \quad 2115001826030741919\zeta^2 + \quad \quad \quad 1131970596131071140\zeta^3 + \quad \quad \quad 2242211081414930646\zeta^4)T^{155} \\ & \cdot (\quad \quad \quad 10794802085997152893\zeta - \quad \quad \quad 125169242094652686197\zeta^2 + \quad \quad \quad 5572271617029639788\zeta^3 - \quad \quad \quad 3578221829410897277\zeta^4)T^{150} \\ & \cdot (- \quad \quad \quad 1092489892026183240595\zeta - \quad \quad \quad 19045894680361532195\zeta^2 - \quad \quad \quad 82493491068698742020\zeta^3 + \quad \quad \quad 1054754437099624148380\zeta^4)T^{145} \\ & \cdot (- \quad \quad \quad 5264940377372808644860\zeta + \quad \quad \quad 7617655486050966135945\zeta^2 - \quad \quad \quad 2208810719148956967200\zeta^3 + \quad \quad \quad 5919675578839593861180\zeta^4)T^{140} \\ & \cdot (\quad \quad \quad 35231126802022906923700\zeta + \quad \quad \quad 76991096784296511267395\zeta^2 - \quad \quad \quad 2844591922704368405660\zeta^3 + \quad \quad \quad 57649409403743947389085\zeta^4)T^{135} \\ & \cdot (- \quad \quad \quad 47078555376988708075719\zeta + \quad \quad \quad 200899198924234951562728\zeta^2 - \quad \quad \quad 178949929296735577625890\zeta^3 + \quad \quad \quad 10038925041345017004512\zeta^4)T^{130} \\ & \cdot (- \quad \quad \quad 31983449855840321598354\zeta + \quad \quad \quad 136172420618496196359621\zeta^2 - \quad \quad \quad 466246706226228978432904\zeta^3 - \quad \quad \quad 346553448466428222999679\zeta^4)T^{125} \\ & \cdot (\quad \quad \quad 1180192067646162748733050\zeta + \quad \quad \quad 205455482183199912333875\zeta^2 - \quad \quad \quad 163763655100212872238575\zeta^3 - \quad \quad \quad 83100189407529085012325\zeta^4)T^{120} \\ & \cdot (\quad \quad \quad 3059963454586358196126275\zeta + \quad \quad \quad 244936329158456058499950\zeta^2 + \quad \quad \quad 545838422257132671468625\zeta^3 + \quad \quad \quad 512501234059197317441050\zeta^4)T^{115} \\ & \cdot (\quad \quad \quad 3979257732937663486439500\zeta + \quad \quad \quad 79225077814751555461450\zeta^2 + \quad \quad \quad 889574860231725659904650\zeta^3 + \quad \quad \quad 254529912494647967785225\zeta^4)T^{110} \\ & \cdot (\quad \quad \quad 3467562297818772888004840\zeta - \quad \quad \quad 85725012712521041603605\zeta^2 + \quad \quad \quad 281055925018219463672875\zeta^3 + \quad \quad \quad 1589569328971771556605\zeta^4)T^{105} \\ & \cdot (\quad \quad \quad 2144173501004116108395965\zeta - \quad \quad \quad 266875875221026877505210\zeta^2 - \quad \quad \quad 289731939484927671235510\zeta^3 + \quad \quad \quad 58416643569308765785065\zeta^4)T^{100} \\ & \cdot (\quad \quad \quad 762273215291235256150100\zeta - \quad \quad \quad 283528664040523758804150\zeta^2 - \quad \quad \quad 358301031221634135630400\zeta^3 - \quad \quad \quad 61868672356522918697150\zeta^4)T^{95} \\ & \cdot (\quad \quad \quad 92450484250738213940925\zeta - \quad \quad \quad 176818574494659617988850\zeta^2 - \quad \quad \quad 176889224147872014607625\zeta^3 - \quad \quad \quad 174206681963141408783400\zeta^4)T^{90} \\ & \cdot (- \quad \quad \quad 40044111178252450781000\zeta - \quad \quad \quad 85737155869841603328100\zeta^2 - \quad \quad \quad 52967312889452485105200\zeta^3 - \quad \quad \quad 142803548699047746983800\zeta^4)T^{85} \\ & \cdot (- \quad \quad \quad 28320121922644518584190\zeta - \quad \quad \quad 36329555220583241551170\zeta^2 - \quad \quad \quad 15370939070058432208925\zeta^3 - \quad \quad \quad 67300961560912082340605\zeta^4)T^{80} \\ & \cdot (- \quad \quad \quad 11317157764194631449965\zeta - \quad \quad \quad 12443611579843256032115\zeta^2 - \quad \quad \quad 6162480797122406437265\zeta^3 - \quad \quad \quad 20813206535815428571040\zeta^4)T^{75} \\ & \cdot (- \quad \quad \quad 3417219276505031827575\zeta - \quad \quad \quad 3166643887326249676825\zeta^2 - \quad \quad \quad 2433483906393330335825\zeta^3 - \quad \quad \quad 4388908591501280154450\zeta^4)T^{70} \\ & \cdot (- \quad \quad \quad 658421946396854279850\zeta - \quad \quad \quad 528616430424494946050\zeta^2 - \quad \quad \quad 650737039623651709250\zeta^3 - \quad \quad \quad 615885744328630532200\zeta^4)T^{65} \\ & \cdot (- \quad \quad \quad 38907578100685411125\zeta - \quad \quad \quad 18883362013022544300\zeta^2 - \quad \quad \quad 80698153065160491225\zeta^3 - \quad \quad \quad 25844018052789803275\zeta^4)T^{60} \\ & \cdot (\quad \quad \quad 12672276508303245799\zeta + \quad \quad \quad 15176377615902722242\zeta^2 + \quad \quad \quad 4789997165491124475\zeta^3 + \quad \quad \quad 14234235783867177438\zeta^4)T^{55} \\ & \cdot (\quad \quad \quad 3203254527174167929\zeta + \quad \quad \quad 3797253764271593439\zeta^2 + \quad \quad \quad 3055155956145585774\zeta^3 + \quad \quad \quad 3885314532490306884\zeta^4)T^{50} \\ & \cdot (\quad \quad \quad 291949745622074780\zeta + \quad \quad \quad 433081185270028705\zeta^2 + \quad \quad \quad 427937400402498905\zeta^3 + \quad \quad \quad 437184792279348330\zeta^4)T^{45} \\ & \cdot (\quad \quad \quad 8015095785609415\zeta + \quad \quad \quad 29250162314242120\zeta^2 + \quad \quad \quad 28785572362552250\zeta^3 + \quad \quad \quad 22607038185282280\zeta^4)T^{40} \\ & \cdot (- \quad \quad \quad 66709042185175\zeta + \quad \quad \quad 1396760816130745\zeta^2 + \quad \quad \quad 1151288328971040\zeta^3 + \quad \quad \quad 418807393258260\zeta^4)T^{35} \\ & \cdot (\quad \quad \quad 8195468724622\zeta + \quad \quad \quad 39045235823931\zeta^2 + \quad \quad \quad 32870511466680\zeta^3 + \quad \quad \quad 4474269099729\zeta^4)T^{30} \\ & \cdot (\quad \quad \quad 1019179484982\zeta + \quad \quad \quad 252468849497\zeta^2 - \quad \quad \quad 459131887583\zeta^3 + \quad \quad \quad 363520052\zeta^4)T^{25} \\ & \cdot (\quad \quad \quad 35724629370\zeta + \quad \quad \quad 10212806845\zeta^2 - \quad \quad \quad 16496176080\zeta^3 - \quad \quad \quad 11902515805\zeta^4)T^{20} \\ & \cdot (\quad \quad \quad 73971560\zeta + \quad \quad \quad 282361655\zeta^2 + \quad \quad \quad 4762200\zeta^3 - \quad \quad \quad 339029280\zeta^4)T^{15} \\ & \cdot (\quad \quad \quad 3599175\zeta + \quad \quad \quad 1610205\zeta^2 + \quad \quad \quad 1159860\zeta^3 + \quad \quad \quad 796965\zeta^4)T^{10} \\ & \cdot (- \quad \quad \quad 3261\zeta + \quad \quad \quad 3957\zeta^2 - \quad \quad \quad 435\zeta^3 - \quad \quad \quad 6447\zeta^4)T^5 \end{aligned}$$

+1

Table 2.

$$\beta = 1 - 5\zeta, N\beta = 11$$

The norm of the prime l	The minimum in N $\equiv \zeta \pmod{l}$	The type of the factors of Ψ and Φ
41	16	<i>irred.</i>
131	61	$(1^5)(25)$
191	184	$(5)(5^5)$
191	49	$(10)(41^5)$
281	90	$(5)^4(10)$
761	684	$(5)(1^5)(4^5)$

$$\beta = 2\zeta - \zeta^2, N\beta = 31$$

The norm of the prime l	The minimum in N $\equiv \zeta \pmod{l}$	The type of the factors of Ψ and Φ
41	37	$(1^5)(85)$
71	54	$(1^5)(5)(80)$
271	187	$(5)^2(10)(35)^2$
281	90	<i>irred.</i>
311	6	$(5)(17^5)$

$$\beta = \zeta^2 + 2\zeta^3 + 3\zeta^4, N\beta = 41$$

The norm of the prime l	The minimum in N $\equiv \zeta \pmod{l}$	The type of the factors of Ψ and Φ
61	3	(24^5)
271	10	$(5)(10)(105)$
281	232	$(5)(115)$
971	803	$(10)(22^5)$
1811	956	$(5)(4^5)(19^5)$

$$\beta = -3\zeta^2 - \zeta^4, N\beta = 61$$

The norm of the prime l	The minimum in N $\equiv \zeta \pmod{l}$	The type of the factors of Ψ and Φ
211	188	$(10)(7^5)(135)$
1231	190	$(5)^2(34^5)$
1291	319	<i>irred.</i>
1831	655	$(1^5)(5)(10)(4^5)(28^5)$
2311	2006	$(1^5)(175)$

- 1) All the cases, the reduced polynomials are separable.
- 2) In the third column, for instance, $(1^5)(5)(10)(4^5)(28^5)$ indicates
 - (a) $\Psi(\beta; S)$ modulo ℓ factors the product of 2 polynomials of degree 1, 1 polynomial of degree 2, 1 polynomial of degree 4 and 1 polynomial of degree 28; furthermore
 - (b) if we substitute T^5 as S , then each factor decomposes respectively the product of 5 polynomials of degree 1, of 1 polynomial of degree 10, of 5 polynomials of degree 4 and of 5 polynomials of degree 28.